Приложение № 1
к приказу ГОАУ «АРНО» от 03.10.2023 № 123

ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
В ГОСУДАРСТВЕННОМ ОБЛАСТНОМ АВТОНОМНОМ УЧРЕЖДЕНИИ
«АГЕНТСТВО РАЗВИТИЯ НОВГОРОДСКОЙ ОБЛАСТИ»

Великий Новгород

ОГЛАВЛЕНИЕ

Раздел I. Основные положения

1. Общие положения

1.1. Настоящая **Политика в отношении обработки персональных данных в государственном областном автономном учреждении «Агентство развития Новгородской области» (далее - Политика)** определяет политику обработки, порядок сбора, учета, накопления, использования, распространения, хранения, уничтожения персональных данных, основные принципы, цели, условия и способы обработки персональных данных, перечни субъектов и обрабатываемых в **государственном областном автономном учреждении «Агентство развития Новгородской области»** (далее - Учреждение) персональных данных, функции Учреждения при обработке персональных данных, права субъектов персональных данных, а также реализуемые в Учреждении требования к защите персональных данных.

1.2. Политика утверждается приказом Учреждения. Политика действует бессрочно после утверждения и до ее замены новой версией. Внесение изменений (дополнений) в Политику, включая приложения к ней, производится Учреждением в одностороннем порядке. Все изменения (дополнения), вносимые Учреждением в Политику, вступают в силу и становятся обязательными с даты подписания приказа об утверждении новой версии Политики.

1.3. Настоящая Политика разработана в соответствии с Конституцией Российской Федерации (РФ), Трудовым кодексом РФ, Гражданским кодексом РФ, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон), Уставом Учреждения и другими правовыми актами в области обработки и защиты персональных данных.

1.4. Положения Политики действуют в отношении всех персональных данных, обрабатываемых Учреждением, в том числе персональных данных, поступающих от пользователей в информационно-телекоммуникационной сети Интернет на сайте Новгородского Центра «Мой бизнес» (https://mb53.ru/) (далее также сайт ЦМБ), а также на официальном сайте Учреждения (http://novgorodinvest.ru/) (далее также сайт). Политика распространяет свое действие на обрабатываемые Учреждением персональные данные, которые были получены как до, так и после ввода в действие настоящей Политики. Порядок обработки персональных данных в Учреждении регулируется настоящей Политикой в соответствии с требованиями действующего законодательства Российской Федерации в области персональных данных.

2. Основные термины, понятия и определения, правовые основания обработки персональных данных

2.1. В настоящей Политике используются следующие основные термины, понятия и определения:

1) **персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

1.1) **персональные данные, разрешенные субъектом персональных данных для распространения,** - персональные данные, доступ неограниченного круга лиц

к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;

2) **оператор** - Учреждение, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

3) **обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

4) **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

5) **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) **уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) **информационная система** – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации с целью решения задач Учреждения;

11) **трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

12) **смешанная обработка персональных данных** – обработка персональных данных с помощью средств автоматизации и без нее;

13) **пользователь** – любое физическое лицо, индивидуальный предприниматель либо представитель юридического лица, посещающий официальный сайт Учреждения (http://novgorodinvest.ru/), посещающий сайт Новгородского Центра «Мой бизнес» (https://mb53.ru/), посещающий официальные страницы Учреждения в социальных сетях.

14) **официальные страницы Учреждения** - персональные страницы Учреждения в социальных сетях (https://vk.com/mybiz53, https://vk.com/investnovgorod), содержащие информацию о своей деятельности (далее также страницы Учреждения).

15) **администратор информационной безопасности** – специалист Учреждения, в должностные обязанности которого входит контроль за обеспечением защиты информации, а также организация работ по выявлению и предупреждению возможных каналов утечки информации, предупреждению потенциального несанкционированного доступа к защищаемой информации.

16) **лица, ответственные за обработку персональных данных** – работники Учреждения, осуществляющие обработку персональных данных и/или получившие доступ к персональным данным.

17) **информационная безопасность** – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов общества в условиях угроз в информационной сфере.

18) **информационные ресурсы** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

19) **Яндекс метрика** - инструмент веб-аналитики, который помогает получать наглядные отчеты, записи действий посетителей, отслеживать источники трафика и оценивать эффективность онлайн- и офлайн-рекламы.

20) **цифровая платформа МСП** - государственная платформа поддержки предпринимателей и тех, кто планирует начать свой бизнес, разработана Корпорацией МСП совместно с Минэкономразвития России с целью — предоставить доступ ко всем необходимым для бизнеса сервисам и мерам поддержки в одном месте (https://мсп.рф) (далее также ЦП МСП).

2.2. Правовым основанием обработки персональных данных является совокупность нормативных правовых актов, во исполнение которых и в соответствии с которыми Учреждение осуществляет обработку персональных данных, в их числе:

Конституция Российской Федерации;

Гражданский кодекс Российской Федерации;

Трудовой кодекс Российской Федерации;

Налоговый кодекс Российской Федерации;

Федеральный закон от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;

Федеральный закон от 12.01.1996 № 7-ФЗ «О некоммерческих организациях»;

Федеральный закон от 24.07.2007 № 209-ФЗ «О развитии малого и среднего предпринимательства в Российской Федерации»;

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Приказ Минэкономразвития России от 14.03.2019 № 125 «Об утверждении Требований к реализации мероприятий, осуществляемых субъектами Российской Федерации, бюджетам которых предоставляются субсидии на государственную поддержку малого и среднего предпринимательства в субъектах Российской

Федерации в целях достижения целей, показателей и результатов региональных проектов, обеспечивающих достижение целей, показателей и результатов федеральных проектов, входящих в состав национального проекта «Малое и среднее предпринимательство и поддержка индивидуальной предпринимательской инициативы», и требований к организациям, образующим инфраструктуру поддержки субъектов малого и среднего предпринимательства»;

Приказ Минэкономразвития России от 26.03.2021 № 142 «Об утверждении требований к реализации мероприятий, осуществляемых субъектами Российской Федерации, бюджетам которых предоставляются субсидии на государственную поддержку малого и среднего предпринимательства, а также физических лиц, применяющих специальный налоговый режим «Налог на профессиональный доход», в субъектах Российской Федерации, направленных на достижение целей, показателей и результатов региональных проектов, обеспечивающих достижение целей, показателей и результатов федеральных проектов, входящих в состав национального проекта «Малое и среднее предпринимательство и поддержка индивидуальной предпринимательской инициативы», и требований к организациям, образующим инфраструктуру поддержки субъектов малого и среднего предпринимательства»;

Распоряжение Правительства Новгородской области от 7 сентября 2017 г. № 281-рг «Об определении специализированной организации по привлечению инвестиций и работе с инвесторами в Новгородской области, функциях, полномочиях и порядке взаимодействия ее с органами исполнительной власти Новгородской области»;

Распоряжение Правительства Новгородской области от 7 сентября 2017 г. № 11-рг от 29.01.2019 «О едином органе управления организациями, образующими инфраструктуру поддержки субъектов малого и среднего предпринимательства Новгородской области»

Приказ Департамента экономического развития Новгородской области от 28 апреля 2017 г. № 42 «Об утверждении Регламента сопровождения инвестиционных проектов, реализуемых и (или) планируемых к реализации на территории Новгородской области по принципу «одного окна»;

иные нормативные правовые акты, регулирующие отношения, связанные с деятельностью Учреждения.

Правовым основанием обработки персональных данных также являются: Устав Учреждения, договоры, заключаемые между Учреждением и субъектами персональных данных, согласие субъектов персональных данных на обработку персональных данных, согласие субъектов персональных данных на распространение персональных данных.

3. Перечень субъектов персональных данных, персональные данные которых обрабатываются в Учреждении

В Учреждении обрабатываются персональные данные следующих категорий субъектов персональных данных:

3.1. Работники Учреждения/работники, ранее состоявшие в трудовых отношениях с оператором, родственники работников/бывших работников.

3.2. Кандидаты на замещение вакантных должностей Учреждения.

3.3. Физические лица, состоящие в гражданских (договорных) отношениях с оператором.

3.4. Представители контрагентов, потенциальных контрагентов (индивидуального предпринимателя, юридического лица) Учреждения.

3.5. Лица, подающие заявки на участие в конкурентных процедурах закупок товаров, работ, услуг.

3.6. Лица, предоставляющие Учреждению коммерческие предложения.

3.7. Лица, обращающиеся в Учреждение с заявлениями/жалобами и их представители.

3.8. Физические лица, планирующие начать предпринимательскую и/или инвестиционную деятельность на территории Новгородской области, физические лица, зарегистрированные в качестве индивидуального предпринимателя, физические лица, применяющие специальный налоговый режим «Налог на профессиональный доход» и осуществляющие деятельность на территории Новгородской области, представители юридических лиц, индивидуальных предпринимателей, обращающиеся в Учреждение за получением услуг, сервисов и мер поддержки, относящимся к компетенции Учреждения.

3.9. Физические лица, индивидуальные предприниматели, представители юридических лиц, обратившиеся в Учреждение для получения услуг, сервисов и мер поддержки в иных организациях и учреждениях, расположенных в Новгородском Центре «Мой Бизнес» (далее ЦМБ).

3.10. Пользователи сайта ЦМБ, сайта Учреждения, страниц Учреждения, ЦП МСП.

4. Принципы и цели обработки персональных данных

4.1. Обработка персональных данных в Учреждении осуществляется с учетом необходимости обеспечения защиты прав и свобод работников Учреждения и иных субъектов персональных данных, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну, на основе следующих принципов:

- обработка персональных данных осуществляется в Учреждении на законной и справедливой основе;
- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;
- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;
- при обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Лица, осуществляющие обработку персональных данных, принимают необходимые меры либо

обеспечивают их принятие по удалению или уточнению неполных или неточных персональных данных;

- обрабатываемые персональные данные уничтожаются либо обезличиваются по достижению целей обработки или в случае утраты необходимости достижения этих целей, если иное не предусмотрено законодательством Российской Федерации;

- соблюдение режима секретности (конфиденциальности) лицами, осуществляющими обработку персональных данных либо имеющими к ним доступ.

4.2. Персональные данные субъектов, предусмотренных п.п. 3.1, 3.2 настоящей Политики, обрабатываются в целях:

- для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

- обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

- обеспечения работникам установленных законодательством Российской Федерации и локальными нормативными актами условий труда, гарантий и компенсаций, а также в целях противодействия коррупции;

- осуществления функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на Учреждение, в том числе по предоставлению персональных данных в органы государственной власти (Фонд пенсионного и социального страхования Российской Федерации, а также иные органы государственной власти и местного самоуправления);

- защиты жизни, здоровья или иных жизненно важных интересов субъектов персональных данных;

- предоставления сведений субъектов в информационные системы, требования по ведению которых установлены нормативными правовыми актами и локальными правовыми актами Учреждения (в том числе в информацию систему Единая общероссийская справочно-информационная система по охране труда, Единая государственная информационная система в сфере здравоохранения и пр.).

4.3. Персональные данные субъектов, предусмотренных п.п. 3.3, 3.4, 3.5, 3.6 настоящей Политики, обрабатываются в целях:

- исполнения договоров, а также для подготовки, заключения и прекращения договоров с контрагентами;

- обеспечения соблюдения требований Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации, локальных нормативных актов Учреждения;

- формирования справочных материалов для внутреннего информационного обеспечения деятельности Учреждения;

- исполнения судебных актов, актов других органов или должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации;

- осуществления прав и законных интересов Учреждения в рамках осуществления видов деятельности, предусмотренных Уставом и иными

локальными нормативными актами Учреждения, или третьих лиц либо достижение общественно значимых целей;

- в иных законных целях для осуществления деятельности, предусмотренной локальными нормативными актами Учреждения.

4.4. Персональные данные субъектов, предусмотренных п. 3.7 настоящей Политики, обрабатываются в целях:

- рассмотрения личных, а также индивидуальных или коллективных письменных обращений или обращений в форме электронного документа с последующим уведомлением заявителей о результатах рассмотрения;

- обеспечения соблюдения требований Федерального закона от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» и иных нормативно-правовых актов в сфере рассмотрения обращений граждан.

4.5. Персональные данные субъектов, предусмотренных п.п. 3.8, 3.9, 3.10 настоящей Политики, обрабатываются в целях:

- оказания Учреждением или привлеченным Учреждением контрагентом услуг, сервисов и мер поддержки лицам, планирующим начать предпринимательскую и/или инвестиционную деятельность на территории Новгородской области, в том числе в иных организациях и учреждениях, расположенных в ЦМБ;

- организации и осуществления процесса сопровождения инвестиционных проектов;

- осуществления функций единого органа управления организациями, образующими инфраструктуру поддержки субъектов малого и среднего предпринимательства на территории Новгородской области;

- организации оказания и предоставления в ЦМБ комплекса услуг, сервисов и мер поддержки субъектам малого и среднего предпринимательства Новгородской области и гражданам, планирующим начать предпринимательскую деятельность, а также физическим лицам, применяющим специальный налоговый режим «Налог на профессиональный доход»;

- вовлечения в предпринимательскую деятельность и содействия созданию собственного бизнеса, включая поддержку создания сообществ начинающих предпринимателей и развитие института наставничества;

- популяризации деятельности Учреждения и получателей услуг;

- обеспечение функционирования сайтов ЦМБ, Учреждения, страниц Учреждения, ЦП МСП, предусматривающих:

экспертную поддержку пользователей по вопросам порядка и условий получения услуг, предоставляемых Учреждением и иными организациями и учреждениями, расположенными в центре «Мой Бизнес» Новгородской области;

формирование заявления (запроса) на услуги Учреждения, в том числе с возможностью направления документов;

установления с пользователем обратной связи, включая направление уведомлений, запросов, касающихся использования сайтов Учреждения и ЦМБ, страниц Учреждения, ЦП МСП, оказания услуг, обработку запросов и заявок от

пользователя, поступивших через сайты Учреждения и ЦМБ, страницы Учреждения, ЦП МСП;

улучшение качества работы сайтов, страниц Учреждения, ЦП МСП, удобства использования, разработка новых сервисов и услуг;

предоставления пользователям возможности участия в мероприятиях, в том числе получения приглашений на мероприятия и т.д.;

ведения истории активности пользователей и истории запросов;

осуществление рекламной деятельности;

регистрацию в личном кабинете пользователя;

предоставления пользователю доступа к персонализированным ресурсам сайта.

Раздел II. Обработка персональных данных

5. Перечень действий с персональными данными и способы их обработки

5.1. Учреждение осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных.

5.2. Обработка персональных данных субъектов персональных данных осуществляется следующими способами: смешанная; с передачей по внутренней сети оператора; с передачей по сети Интернет.

5.3. Хранение персональных данных в Учреждении осуществляется:

- в программах бухгалтерского, финансового, складского, кадрового учета, в т.ч. 1С, СЭД «Дело»;
- в файловом хранилище на сетевом диске с закрытым доступом;
- информационная система ЦП МСП, сайты, страницы Учреждения;
- на бумажном носителе.

6. Общие условия и порядок обработки персональных данных

6.1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных действующим законодательством Российской Федерации и локальными нормативными актами Учреждения. Обработка персональных данных должна ограничиваться достижением целей их обработки.

6.2. Учреждение предупреждает об обработке персональных данных следующими способами:

- на сайтах Учреждения, ЦМБ субъекту предоставляется ознакомление с утвержденной Учреждением Политикой конфиденциальности в области обработки и обеспечения безопасности персональных данных, обрабатываемых в сети Интернет на информационных ресурсах государственного областного автономного учреждения «Агентство развития Новгородской области»;
- при телефонном звонке в Учреждение (по номеру 8-800-550-11-88 или (88162) 50 19 90) голосовое предупреждение об обработке персональных данных с использованием функции автоответчика.

6.3. Обработка персональных данных должна осуществляться с согласия субъекта персональных данных на обработку его персональных данных, за

исключением случаев, предусмотренных действующим законодательством Российской Федерации и локальными нормативными актами Учреждения.

6.4. Сотрудники Учреждения, обрабатывающие персональные данные и/или получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом.

6.5. В целях внутреннего информационного обеспечения деятельности Учреждения могут создаваться внутренние справочные материалы, в которые с письменного согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, могут включаться его фамилия, имя, отчество, число, месяц и год рождения, место работы, должность, адрес электронной почты, контактный телефон и проч.

6.6. Обработка и/или доступ к обрабатываемым в Учреждении персональным данным разрешается только сотрудникам Учреждения, входящим в утвержденный в Учреждении список сотрудников, имеющих доступ к персональным данным для выполнения служебных (трудовых) обязанностей. Помимо указанных лиц доступ к персональным данным имеют только лица, уполномоченные действующим законодательством.

6.7. Запрещается получать, обрабатывать персональные данные субъектов персональных данных, не предусмотренные настоящей Политикой, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

6.8. Обработка биометрических персональных данных (фотографии, видеообраз) должна осуществляться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных Федеральным законом.

6.9. Обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 Федерального закона.

6.10. Если предоставление персональных данных является обязательным в соответствии с действующим законодательством Российской Федерации, лицо, обрабатывающее персональные данные, обязано разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

6.11. Если персональные данные получены не от субъекта персональных данных, лицо, обрабатывающее персональные данные, за исключением случаев, предусмотренных в п. 6.12 настоящей Политике, до начала обработки таких персональных данных обязано предоставить субъекту персональных данных следующую информацию:

наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

цель обработки персональных данных и ее правовое основание;

перечень персональных данных;

предполагаемые пользователи персональных данных;

установленные Федеральным законом права субъекта персональных данных;

источник получения персональных данных.

6.12. Лицо, обрабатывающее персональные данные, освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные п. 6.11 настоящей Политики, в случаях, если:

субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

персональные данные получены оператором на основании Федерального закона или в связи с исполнением договора, по которому субъект персональных данных является выгодоприобретателем или поручителем;

обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 Федерального закона;

оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

предоставление субъекту персональных данных сведений, предусмотренных п. 6.11 настоящей Политики, нарушает права и законные интересы третьих лиц.

6.13. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных лицо, обрабатывающее персональные данные, обязано осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных лицо, обрабатывающее персональные данные, обязано осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

6.14. В случае подтверждения факта неточности персональных данных лицо, обрабатывающее персональные данные, на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязано уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

6.15. В случае выявления неправомерной обработки персональных данных, осуществляемой лицом, обрабатывающим персональные данные, такое лицо в срок, не превышающий трех рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, лицо, обрабатывающее персональные данные, в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязано уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных лицо, обрабатывающее персональные данные, обязано уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта

персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

6.16. В случае достижения цели обработки персональных данных лицо, обрабатывающее персональные данные, обязано прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, по которому субъект персональных данных является выгодоприобретателем или поручителем, иным соглашением между Учреждением и субъектом персональных данных либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных действующим законодательством Российской Федерации.

6.17. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных лицо, обрабатывающее персональные данные, обязано прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, по которому субъект персональных данных является поручителем или выгодоприобретателем, иным соглашением между Учреждением и субъектом персональных данных либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных действующим законодательством Российской Федерации.

6.18. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в п.п. 6.15 – 6.17 настоящей Политики, лицо, обрабатывающее персональные данные, осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

7. Условия и порядок обработки персональных данных субъектов, предусмотренных п.п. 3.1, 3.2 настоящей Политики

7.1. В целях, указанных в пункте 4.2 настоящей Политики, обрабатываются следующие категории персональных данных:

фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

число, месяц, год рождения;

место рождения;

информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

адрес места жительства (адрес регистрации, фактического проживания);

номер контактного телефона или сведения о других способах связи;

реквизиты страхового свидетельства государственного пенсионного страхования;

идентификационный номер налогоплательщика;

реквизиты свидетельства государственной регистрации актов гражданского состояния;

семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);

биографические и анкетные данные работника, результаты тестирований, прохождения конкурсов, сдачи экзаменов;

сведения о трудовой деятельности;

сведения о воинском учете и реквизиты документов воинского учета;

сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);

сведения о профессии;

сведения об ученой степени;

информация о владении иностранными языками, степень владения;

медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего принятию на работу и работе по должности (профессии, специальности);

фотография;

сведения о социальных льготах;

сведения о прохождении государственной гражданской службы;

информация о наличии или отсутствии судимости;

государственные награды, иные награды и знаки отличия;

сведения о профессиональной переподготовке и (или) повышении квалификации;

информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;

сведения о доходах, об имуществе и обязательствах имущественного характера;

номер расчетного счета;

номер банковской карты;

биометрические данные (фотография, видеообраз)

иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 4.2 настоящей Политики.

7.2. Обработка персональных данных субъектов, предусмотренных п.п. 3.1, 3.2 настоящей Политики, осуществляется при условии получения согласия указанных лиц в следующих случаях:

- при передаче (распространение, предоставление, доступ) персональных данных третьим лицам в случаях, не предусмотренных действующим законодательством Российской Федерации;

- при трансграничной передаче персональных данных;

- при принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

7.3. В случаях, предусмотренных пунктом 7.2. настоящей Политики, согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом.

7.4. Обработка персональных данных субъектов, предусмотренных п.п. 3.1, 3.2

настоящей Политики, включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных.

Лица, осуществляющие обработку персональных данных либо имеющие к ним доступ, обязаны соблюдать режим секретности (конфиденциальности).

7.5. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов, предусмотренных п.п. 3.1, 3.2 настоящей Политики осуществляется путем:

- получения оригиналов необходимых документов (заявление, трудовая книжка, автобиография и иные);
- внесения сведений в учетные формы (на бумажных и электронных носителях);
- формирования персональных данных в ходе работы;
- внесения персональных данных в информационные системы Учреждения.

7.6. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от указанных субъектов персональных данных.

7.7. В случае возникновения необходимости получения персональных данных работников Учреждения и кандидатов на замещение вакантных должностей Учреждения, у третьей стороны, следует известить об этом работников Учреждения и кандидатов на замещение вакантных должностей Учреждения заранее, получить их письменное согласие и сообщить им о целях, предполагаемых источниках и способах получения персональных данных, а также характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

7.8. Запрещается получать, обрабатывать персональные данные субъектов, предусмотренных п.п. 3.1, 3.2 настоящей Политики, не предусмотренные пунктом 7.1 настоящей Политики, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

7.9. Передача (распространение, предоставление, доступ) и использование персональных данных субъектов, предусмотренных п.п. 3.1, 3.2 настоящей Политики, осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

7.10. Не требуется согласие сотрудника на передачу его персональных данных:

- третьим лицам в целях предупреждения угрозы жизни и здоровью работника;
- в Фонд пенсионного и социального страхования Российской Федерации в объеме, предусмотренном действующим законодательством Российской Федерации;
- в налоговые органы;
- в военные комиссариаты;
- по мотивированному запросу органов прокуратуры, правоохранительных органов и органов безопасности, судебных органов;
- по запросу от государственных инспекторов труда при осуществлении ими надзорно-контрольной деятельности;
- в случаях, связанных с исполнением сотрудником должностных обязанностей;
- в кредитную организацию, обслуживающую платежные карты сотрудников;
- в иных предусмотренных федеральными законами случаях.

8. Условия и порядок обработки персональных данных субъектов, предусмотренных п.п. 3.3, 3.4, 3.5, 3.6. настоящей Политики

8.1. В целях, указанных в пункте 4.3 настоящей Политики, обрабатываются следующие категории персональных данных:

фамилия, имя, отчество;

число, месяц, год, место рождения;

вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

адрес места жительства (адрес регистрации, фактического проживания);

реквизиты страхового свидетельства государственного пенсионного страхования;

идентификационный номер налогоплательщика;

номер расчетного счета;

номер банковской карты;

сведения об образовании (наименование и год окончания образовательной организации, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);

сведения о месте работы, о занимаемой должности, об опыте работы;

адреса электронной почты, номера контактных телефонов;

иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 4.3 настоящей Политики.

8.2. Обработка персональных данных субъектов, предусмотренных п.п. 3.3, 3.4, 3.5, 3.6 настоящей Политики включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных.

8.3. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов, предусмотренных пп. 3.3, 3.4, 3.5, 3.6 настоящей Политики, осуществляется путем:

- получения оригиналов необходимых документов;
- копирования оригиналов документов;
- внесения сведений в учетные формы (на бумажных и электронных носителях);
- формирования персональных данных в ходе работы;
- внесения персональных данных в информационные системы Учреждения.

9. Условия и порядок обработки персональных данных субъектов, предусмотренных п. 3.7 настоящей Политики

9.1. В целях, указанных в пункте 4.4 настоящей Политики, обрабатываются следующие категории персональных данных:

фамилия, имя, отчество;

почтовый адрес, место жительства;

адрес электронной почты;

указанный в обращении контактный телефон;

иные персональные данные, указанные заявителем в обращении (жалобе), а также ставшие известными в ходе личного приема или в процессе рассмотрения поступившего обращения.

9.2. Обработка персональных данных, необходимых для достижения целей, указанных в пункте 4.4 настоящей Политики, осуществляется без согласия

субъектов персональных данных в соответствии с пунктом 4 части 1 статьи 6 Федерального закона.

9.3. Обработка персональных данных включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных.

9.4. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов, обратившихся в Учреждение с заявлением/обращением/жалобы, осуществляется путем:

- получения необходимых документов (заявление/обращение/жалоба);
- внесения сведений в учетные формы (на бумажных и электронных носителях).

9.5. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от субъектов персональных данных (заявителей).

9.6. При предоставлении заявления/обращения/жалобы Учреждению запрещается запрашивать у субъектов персональных данных и третьих лиц, а также обрабатывать персональные данные в случаях, не предусмотренных законодательством Российской Федерации.

9.7. Передача (распространение, предоставление) и использование персональных данных заявителей (субъектов персональных данных) осуществляется лишь в случаях и в порядке, предусмотренных законодательством Российской Федерации.

10. Условия и порядок обработки персональных данных субъектов, предусмотренных п.п. 3.8, 3.9, 3.10 настоящей Политики

10.1. В целях, указанных в пункте 4.5 настоящей Политики, обрабатываются следующие категории персональных данных:

фамилия, имя, отчество;

число, месяц, год, место рождения;

вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

адрес места жительства (адрес регистрации, фактического проживания);

номер контактного телефона, электронная почта или сведения о других способах связи;

реквизиты страхового свидетельства государственного пенсионного страхования;

идентификационный номер налогоплательщика;

номер расчетного (лицевого) счета;

номер банковской карты;

сведения об образовании (наименование и год окончания образовательной организации, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);

биометрические персональные данные (фотография, видеообраз);

сведения о месте работы, о занимаемой должности, об опыте работы;

социальное положение, состав семьи;

иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 4.5 настоящей Политики.

10.2. Обработка персональных данных субъектов, предусмотренных п.п. 3.8, 3.9, 3.10 настоящей Политики, включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных.

10.3. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов, предусмотренных п.п. 3.8, 3.9, 3.10 настоящей Политики, осуществляется путем:

- предоставления в устной форме;
- получения оригиналов необходимых документов;
- копирования оригиналов документов;
- внесения сведений в учетные формы (на бумажных и электронных носителях);
- формирования персональных данных в ходе работы;
- внесения персональных данных в информационные системы Учреждения;
- заполнение персональных данных на сайтах Учреждения, страницах Учреждения, ЦП МСП.

11. Порядок обработки персональных данных субъектов персональных данных в информационных системах. Политика информационной безопасности в Учреждении

11.1. Политика информационной безопасности в Учреждении (далее Политика ИБ, информационная безопасность) определяет совокупность правил, требований и руководящих принципов в области информационной безопасности, при работе с персональными данными, которыми руководствуются Учреждение в своей деятельности. Политика ИБ реализуется посредством административно-организационных мер, физических и программно-технических средств.

Персональные данные, которые обрабатываются в информационных системах, подлежат защите от несанкционированного доступа и копирования. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

11.2. Обеспечение безопасности персональных данных в информационных системах и организация обработки персональных данных в информационных системах возлагается на администратора информационной безопасности Учреждения. Ответственность за разработку мер и контроль обеспечения защиты информации несёт администратор информационной безопасности.

Ответственность за реализацию ИБ в Учреждении возлагается:

в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты, а также доведения Политики ИБ до сотрудников Учреждения – на администратора информационной безопасности;

в части, касающейся исполнения Политики ИБ – на каждого сотрудника Учреждения согласно должностным и функциональным обязанностям, и иных лиц, попадающих под область действия Политики ИБ Учреждения.

Руководитель Учреждения несет ответственность за обеспечение выполнения

требований ИБ в Учреждении. Сотрудники Учреждения обязаны соблюдать порядок работы с информационными системами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования Политики ИБ и других документов информационной безопасности.

11.3. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах Учреждения, достигается путем принятия следующих мер по обеспечению безопасности:

определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных Учреждения, формирование на их основе модели угроз;

разработка на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

проверка готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

установка и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Учреждения, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

учет машинных носителей персональных данных;

учет лиц, допущенных к работе с персональными данными в информационной системе;

контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

описание системы защиты персональных данных;

оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

своевременное обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;

установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных Учреждения, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных Учреждения;

осуществление постоянного контроля за обеспечением уровня защищенности персональных данных, за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных;

иные меры, направленные на обеспечение защиты персональных данных, обрабатываемых в информационных системах Учреждения.

11.4. Сотрудникам Учреждения, имеющим право осуществлять обработку персональных данных в информационных системах Учреждения, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе Учреждения.

11.5. Организация ознакомления сотрудников Учреждения в области информационной безопасности возлагается на администратора информационной безопасности. Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по информационной безопасности». Обучение сотрудников правилам обращения с конфиденциальной информацией, проводится путем:

- проведения администратором информационной безопасности инструктивных занятий с сотрудниками, принимаемыми на работу;

- самостоятельного изучения сотрудниками локальных нормативных актов Учреждения.

Допуск сотрудников к работе с содержащейся в информационных базах данных информацией Учреждения осуществляется только после ознакомления с настоящей Политикой ИБ, иными инструкциями пользователей отдельных информационных систем. Согласие на соблюдение правил и требований Политики ИБ подтверждается подписями сотрудников в «Журнале проведения инструктажа по информационной безопасности». Правила допуска к работе с информационными ресурсами лиц, не являющихся сотрудниками, определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

11.6. Каждому сотруднику, допущенному к работе с конкретным информационным ресурсом, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в информационной системе. В случае необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе в информационных системах Учреждения одного и того же имени пользователя («группового имени») запрещено.

11.7. При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение сотрудника) учетная запись должна немедленно блокироваться. Предпочтительно использовать

механизмы автоматического блокирования учетных записей уволенных сотрудников. При невозможности автоматического блокирования учетных записей, администратором информационной безопасности составляется заявка на блокировку учетной записи. В случае необходимости сохранения персональных документов (профайла пользователя) на автоматизированном рабочем месте сотрудника, после прекращения срока действия его полномочий, непосредственный руководитель должен своевременно подать заявку на блокирование учетной записи пользователя с указанием потребности в сохранении данных.

11.8. Регистрационные учетные записи подразделяются: пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов; системные – используемые для нужд операционной системы; служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений. Каждому пользователю информационных ресурсов назначается уникальная пользовательская регистрационная учетная запись. Допускается более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий). В общем случае запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

11.9. Личные пароли должны создаваться пользователями самостоятельно. Длина пароля должна быть не менее 8 символов. В составе пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы. Пароль не должен включать в себя легко вычисляемые сочетания символов (например, «112», «911» и т.п.), а также общепринятые сокращения (например, «ЭВМ», «ЛВС», «USER» и т.п.). Пароль не должен содержать имя учетной записи пользователя или наименование его автоматизированного рабочего места, а также какую-либо его часть, не должен основываться на именах и датах рождения, кличек домашних животных, номеров автомобилей, телефонов и прочих открытых данных о пользователе. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в квартал. В случае компрометации личного пароля пользователя надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или пароля.

11.10. При работе с парольной защитой пользователям запрещается: разглашать кому-либо персональный пароль и прочие идентифицирующие сведения; предоставлять доступ от своей учетной записи посторонним лицам; записывать пароли на бумаге, файле, электронных и прочих носителях информации.

При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

11.11. Контроль за действиями сотрудников Учреждения при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на администратора информационной безопасности. Пользователь несет персональную ответственность за сохранность данных аутентификации (персонального логина и пароля) к автоматизированному рабочему месту и к информационной системе.

11.12. К использованию в Учреждении допускаются только лицензионные и сертифицированные антивирусные средства отечественной разработки. Установка антивирусного ПО производится индивидуально на каждое автоматизированное

рабочее место с обязательным включением настроек от изменения паролем. Пользователям запрещается отключать средства антивирусной защиты и самостоятельно вносить изменения в настройки антивирусного ПО. Настройка параметров средств антивирусного контроля осуществляется администратором информационной безопасности в соответствии руководством по применению конкретного антивирусного программного обеспечения. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должно проводиться обновление антивирусных баз через сеть Интернет с сайта разработчика антивирусных средств или иным доступным способом. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель). Устанавливаемое (изменяемое) ПО должно быть предварительно проверено на отсутствие программ вирусов и других вредоносных модулей. Непосредственно после установки (изменения) ПО рабочих станций и серверов должна быть выполнена антивирусная проверка. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т. п.) сотрудник самостоятельно должен провести антивирусный контроль своей рабочей станции антивирусным сканером. При необходимости – привлечь администратора информационной безопасности для определения факта наличия или отсутствия компьютерного вируса. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники обязаны: приостановить работу; немедленно поставить в известность о факте обнаружения зараженных вирусом файлов, владельца зараженных файлов, а также сотрудников, использующих эти файлы в работе.

Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований, изложенных в настоящем пункте, возлагается на всех сотрудников.

11.13. Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр, не допущенными к ней лицами. При любом оставлении автоматизированного рабочего места (далее также АРМ), рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, заперты в помещении, шкафу или ящике стола или в сейфе. Несанкционированное использование печатающих, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа. Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей должен быть ограничен. Право на доступ к подобным компонентам предоставлено только администратору информационной безопасности. Конечным пользователям предоставляется доступ только к тем

командам, которые необходимы для выполнения их должностных обязанностей. Доступ к информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей. Пользователям запрещается устанавливать неавторизованные программы на компьютеры. Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неавторизованных программ. Техническое обслуживание должно осуществляться только на основании обращения пользователя к системному администратору. Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя. При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений. Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации (в том числе в составе АРМ) допускаются только с санкции пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ. Программное обеспечение должно устанавливаться со специальных ресурсов или съемных носителей и в соответствии с лицензионным соглашением с его правообладателем. Конфигурации устанавливаемых рабочих станций должны быть стандартизованы, а процессы установки, настройки и ввода в эксплуатацию – регламентированы. Автоматизированные рабочие места, на которых предполагается обрабатывать конфиденциальную информацию, должны быть закреплены за соответствующими сотрудниками Учреждения. Запрещается использование указанных АРМ другими пользователями без согласования с администратором информационной безопасности Учреждения. При передаче указанного АРМ другому пользователю, должна производиться гарантированная очистка диска (форматирование).

11.14. Профилактика нарушений Политики информационной безопасности - проведение регламентных работ по защите информации, предупреждение возможных нарушений информационной безопасности и проведение разъяснительной работы по информационной безопасности среди пользователей. Проведение в информационных системах регламентных работ по защите информации предполагает выполнение процедур контрольного тестирования (проверки) функций средств защиты информации, что гарантирует ее работоспособность с точностью до периода тестирования. Контрольное тестирование функций средств защиты информации может быть частичным или полным и должно проводиться с установленной степенью периодичности. Задача предупреждения возможных нарушений информационной безопасности решается по мере наступления следующих событий: включение в состав информационной системы новых программных и технических средств (новых рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в средствах защиты информации информационных систем; изменение конфигурации программных и технических средств информационных систем (изменение конфигурации программного обеспечения рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в средствах защиты информации информационных систем; при появлении сведений о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения технических средств, используемых в

информационных системах. Администратор информационной безопасности (возможно, при помощи сторонней организации специализирующейся в области информационной безопасности) собирает и анализирует информацию о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения относительно информационных систем. Источниками подобного рода сведений могут служить официальные издания и публикации различных компаний, общественных объединений и других организаций, специализирующихся в области защиты информации, рекомендации Управления ФСТЭК по СЗФО, Управления ФСБ по Новгородской области, Министерства Цифрового развития и информационно коммуникационных технологий Новгородской области. Администратор информационной безопасности (возможно, при помощи сторонней организации, специализирующейся в области информационной безопасности) организовывает периодическую проверку средств защиты информации путем моделирования возможных попыток осуществления несанкционированного доступа к защищаемым информационным ресурсам. Плановая разъяснительная работа по правилам Политики ИБ, а также инструктаж сотрудников Учреждения по соблюдению требований ИБ, проводится администратором информационной безопасности;

Внеплановая разъяснительная работа по правилам Политики ИБ, а также инструктаж сотрудников по соблюдению требований нормативных и регламентных документов по информационной безопасности, проводится при пересмотре Политики ИБ, или возникновении инцидента нарушения правил Политики ИБ. Прием на работу новых сотрудников должен сопровождаться ознакомлением их с требованиями Политики ИБ.

11.15. Администратор информационной безопасности, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации информационных систем, должен своевременно обнаруживать нарушения информационной безопасности, факты осуществления несанкционированного доступа к защищаемым информационным ресурсам и предпринимать меры по их локализации и устранению. В случае обнаружения факта нарушения информационной безопасности или осуществления несанкционированного доступа к защищаемым информационным ресурсам рекомендуется уведомить администратора информационной безопасности и/или руководителя Учреждения. После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности информационной системы, а также зарегистрировать факт нарушения в журнале учета событий в сфере защиты персональных данных (приложение № 1 к Политике).

11.16. Ответственность за нарушение правил Политики ИБ несут сотрудники Учреждения в рамках своих служебных обязанностей и полномочий. На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования Политики ИБ, могут быть подвергнуты дисциплинарным взысканиям. Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный Учреждению в результате нарушения ими правил Политики ИБ (ст. 238 Трудового кодекса РФ).

11.17. Обмен персональными данными при их обработке в информационных системах персональных данных Учреждения осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

11.18. Условия прекращения обработки персональных данных оператором:

- достижение целей обработки персональных данных;
- утрата правовых оснований обработки персональных данных;
- прекращение трудовых (договорных) отношений;
- истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных;
- выявление неправомерной обработки персональных данных.

11.19. При увольнении сотрудника, имеющего доступ к персональным данным, или прекращении доступа к персональным данным, документы и иные носители, содержащие персональные данные, сдаются сотрудником своему непосредственному руководителю.

Раздел III. Защита персональных данных

12. Права субъектов персональных данных

12.1. Субъекты персональных данных имеют право на полную информацию об их персональных данных, обрабатываемых в Учреждении, в том числе содержащую:

подтверждение факта обработки персональных данных Учреждением;

правовые основания и цели обработки персональных данных;

цели и применяемые Учреждением способы обработки персональных данных;

наименование и место нахождения Учреждения, сведения о лицах (за исключением работников Учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением или на основании Федерального закона;

обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

сроки обработки персональных данных, в том числе сроки их хранения;

порядок осуществления субъектом персональных данных прав, предусмотренных действующим законодательством Российской Федерации;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения, если обработка поручена или будет поручена такому лицу;

иные сведения, предусмотренные действующим законодательством Российской Федерации.

12.2. Субъекты персональных данных имеют право на доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренным законодательством Российской Федерации.

12.3. Субъекты персональных данных имеют право на уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

12.4. Субъекты персональных данных имеют право на отзыв согласия на обработку персональных данных, в том числе разрешенных субъектом персональных данных для распространения.

12.5. Субъекты персональных данных имеют право на осуществление иных прав, предусмотренных законодательством Российской Федерации.

12.6. Сведения, указанные в п. 12.1 настоящей Политики, должны быть предоставлены субъекту персональных данных Учреждением в доступной форме и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

12.7. Сведения, указанные в п. 12.1 настоящей Политике, предоставляются субъекту персональных данных или его представителю Учреждением при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать реквизиты документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Учреждением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Учреждением, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

12.8. В случае, если сведения, указанные в п. 12.1 настоящей Политики, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Учреждению или направить ему повторный запрос в целях получения сведений, указанных в п. 12.1 настоящей Политики, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен Федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

12.9. Оператор обязан сообщить в порядке, предусмотренном настоящим разделом Политики, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

12.10. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

12.11. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными

данными, относящимися к этому субъекту персональных данных.

12.12. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

12.13. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

12.14. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

12.15. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с

даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

12.16. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

12.17. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в п.п. 12.14 – 12.16 настоящей Политики, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

13. Меры, принимаемые Учреждением для обеспечения выполнения обязанностей оператора при обработке персональных данных

13.1. Меры, необходимые и достаточные для обеспечения выполнения Учреждением обязанностей оператора, предусмотренных законодательством Российской Федерации в области обработки персональных данных, включают:

- назначение лица, ответственного за организацию обработки персональных данных в Учреждении;
- принятие локальных нормативных актов в области обработки и защиты персональных данных;
- принятие локальных нормативных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- получение согласий субъектов персональных данных на обработку персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации;
- обособление персональных данных, обрабатываемых без использования средств автоматизации, от иной информации, в частности, путем их фиксации на отдельных материальных носителях персональных данных, в специальных разделах;

- обеспечение раздельного хранения персональных данных и их материальных носителей, обработка которых осуществляется в разных целях и которые содержат разные категории персональных данных;

- установление запрета на передачу персональных данных по открытым каналам связи, вычислительным сетям вне пределов контролируемой зоны, в сети Интернет без применения установленных в Учреждении мер по обеспечению безопасности персональных данных (за исключение общедоступных и (или) обезличенных персональных данных);

- хранение материальных носителей персональных данных с соблюдением условий, обеспечивающих их сохранность и исключающих несанкционированный доступ к ним (хранение персональных данных в закрытых шкафах, ящиках, сейфах);

- защита паролем автоматизированного рабочего места с персональными данными;

- использование системы паролей при работе в сети;

- осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политики, локальным нормативным актам Учреждения;

- иные меры, предусмотренные законодательством Российской Федерации в области обработки персональных данных.

13.2. Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются в соответствии с требованиями законодательных и иных нормативных правовых актов Российской Федерации, локальных нормативных актов Учреждения, регламентирующих вопросы обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Учреждения.

13.3. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано организовывать:

- внутренний контроль за соблюдением работниками Учреждения законодательства Российской Федерации в области обработки персональных данных, в том числе требований к защите персональных данных;

- доведение до сведения работников Учреждения положений законодательства Российской Федерации, локальных нормативных актов Учреждения в области обработки персональных данных, в том числе требований к защите персональных данных;

- контроль за приемом и обработкой обращений и запросов субъектов персональных данных или их представителей.

13.4. Оператор осуществляет трансграничную передачу персональных данных при условии:

13.4.1. Оператор до начала осуществления трансграничной передачи персональных данных обязан убедиться в том, что иностранным государством, на территорию которого предполагается осуществлять передачу персональных данных, обеспечивается надежная защита прав субъектов персональных данных.

13.4.2. Трансграничная передача персональных данных на территории иностранных государств, не отвечающих вышеуказанным требованиям, может осуществляться только в случае наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных

и/или исполнения договора, стороной которого является субъект персональных данных.

14. Контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов Учреждения в области обработки персональных данных, в том числе требований к защите персональных данных

14.1. Контроль за соблюдением Учреждением законодательства Российской Федерации, локальных нормативных актов в области обработки персональных данных, в том числе требований к защите персональных данных, осуществляется с целью оценки общего состояния выполнения требований по обработке и защите персональных данных в Учреждении, выявления и предотвращения нарушений законодательства в сфере персональных данных, оценки уровня осведомленности и знаний сотрудников Учреждения в области обработки и защиты персональных данных.

14.2. Проверки осуществляются назначаемой приказом руководителя Учреждения комиссией по осуществлению внутреннего контроля за соблюдением законодательства о защите персональных данных (далее - комиссия по проведению внутренних проверок как непосредственно на месте обработки персональных данных путём опроса и осмотра рабочих мест лиц, участвующих в процессе обработки персональных данных, так и путём направления запросов и рассмотрения документов, необходимых для осуществления внутреннего контроля.

14.3. Проверки соответствия обработки и защиты персональных данных установленным требованиям разделяются на плановые и внеплановые.

14.4. Плановые проверки соответствия обработки персональных данных установленным требованиям проводятся не реже одного раза в год в Учреждении. Плановые проверки проводятся в соответствии с Планом проведения внутренних контрольных мероприятий в Учреждении, который формируется председателем комиссии по проведению внутренних проверок и утверждается директором Учреждения.

14.5. План проведения внутренних контрольных мероприятий составляется в декабре текущего года на следующий год, при необходимости может корректироваться. План проведения внутренних контрольных мероприятий (как плановых, так и внеплановых) включает следующие сведения: описание контрольных мероприятий, привлекаемые для проведения контрольных мероприятий сотрудники, сроки проведения контрольных мероприятий.

14.6. По итогам проведения плановых и внеплановых контрольных мероприятий составляет акт, в котором указывается:

описание проведенных мероприятий;

перечень и описание выявленных нарушений при их наличии, рекомендации по их устранению;

заключение по итогам проведения внутреннего контрольного мероприятия.

Общая информация о проведенном контрольном мероприятии фиксируется в журнале учета событий в сфере защиты персональных данных (приложение №1 к настоящей Политике).

Акт проведения внутренней проверки подписывается членами комиссии и утверждается председателем комиссии по проведению внутренних проверок.

14.7. Акты проведения внутренней проверки хранятся у председателя комиссии

по проведению внутренних проверок в течение текущего года. Уничтожение актов проведения внутренней проверки проводится в январе следующего за отчётным года.

14.8. Внеплановые проверки проводятся на основании решения комиссии по проведению внутренних проверок в следующих случаях:

- по результатам расследования выявленных нарушений требований законодательства в сфере защиты персональных данных;
- по результатам внешних контрольных мероприятий, проводимых регулирующими органами;
- по решению руководителя Учреждения.

14.9. Общий срок внутренней проверки не должен превышать 10 (десяти) рабочих дней. При необходимости срок проведения проверки может быть продлён, но не более чем на 10 (десять) рабочих дней.

14.10. В отношении персональных данных, ставших известными в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность.

14.11. Комиссия по проведению внутренних проверок для реализации своих полномочий имеет право: запрашивать у сотрудников Учреждения, имеющих доступ к персональным данным, необходимую информацию; принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемых с нарушением требований действующего законодательства, а также устранению выявленных нарушений выполнения требований к защите персональных данных в Учреждении; вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке; вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в области обработки персональных данных.

15. Сроки обработки и хранение персональных данных

15.1. Персональные данные субъектов персональных данных хранятся в Учреждении до достижения целей обработки.

15.2. Сроки обработки и хранения персональных данных, предоставляемых субъектами персональных данных в Учреждение, определяются нормативными правовыми актами, регламентирующими порядок их сбора, обработки, хранения и уничтожения.

15.3. Персональные данные субъектов персональных данных, содержащиеся в документах, подлежащих хранению в соответствии с требованиями Федерального закона от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации», подлежат хранению в течение срока, установленного вышеуказанным законом.

15.4. Персональные данные, зафиксированные на бумажных носителях, хранятся в запираемых шкафах либо в запираемых помещениях с ограниченным правом доступа, в архивах в соответствии с номенклатурой дел Учреждения. Запрещается хранить документы с персональными данными и их копии на рабочих местах и (или) в открытом доступе, оставлять шкафы (сейфы) открытыми в случае выхода работника из рабочего помещения.

15.5. Персональные данные, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках), возможно и на

разных материальных носителях, с закрытым доступом (с установлением пароля).

15.6. Срок хранения персональных данных, внесенных в информационные системы Учреждения, должен соответствовать сроку хранения бумажных оригиналов.

15.7. Персональные данные субъектов, предусмотренных настоящей Политикой, хранятся в структурных подразделениях, их обрабатывающих с последующим уничтожением либо передачей в порядке, предусмотренном действующим законодательством Российской Федерации и локальными нормативными актами, в архив Учреждения или государственный архив для хранения в соответствии с требованиями действующего законодательства.

15.8. Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляют начальники (руководители) отделов Учреждения согласно их функционалу.

15.9. Учреждение обеспечивает безопасное хранение персональных данных, в том числе:

- соблюдение требований нормативных документов, устанавливающих правила хранения конфиденциальных сведений;

- сохранность имеющихся данных, ограничение доступа к ним, в соответствии с законодательством Российской Федерации и настоящей Политикой;

- контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений;

- хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.

15.10. Места хранения персональных данных на материальных носителях определяются приказом руководителя Учреждения.

16. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

16.1. Сотрудниками, обрабатывающими персональные данные и/или имеющими доступ к персональным данным, осуществляется систематический контроль и выделение документов, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению.

16.2. Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается на заседании комиссии по проведению внутренних проверок Учреждения.

По итогам заседания составляются соответствующие документы об уничтожении документов.

16.3. В случае, если обработка персональных данных осуществляется оператором без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных.

В случае, если обработка персональных данных осуществляется оператором с использования средств автоматизации, документами, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в информационной системе персональных данных (далее – выгрузка из журнала).

В случае, если обработка персональных данных осуществляется оператором одновременно с использованием средств автоматизации и без использования средств автоматизации, документами, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных и выгрузка из журнала.

Акт об уничтожении персональных данных и выгрузка из журнала должны соответствовать требованиям, установленным уполномоченным органом по защите прав субъектов персональных данных.

16.4. Акт об уничтожении персональных данных и выгрузка из журнала подлежат хранению в течение 3 лет с момента уничтожения персональных данных.

16.5. Уничтожение документов, содержащих персональные данные, производится:

- при достижении целей их обработки;

- по решению субъекта персональных данных (при утрате необходимости в достижении целей обработки);

- при достижении окончания срока хранения персональных данных.

При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку, персональные данные подлежат уничтожению в срок, не превышающий 30 дней с даты достижения целей обработки либо утраты необходимости в их достижении, если:

– иное не предусмотрено договором, стороной которого является субъект персональных данных;

– иное не предусмотрено иным соглашением между оператором и субъектом персональных данных.

В случае отзыва субъектом персональных данных согласия на обработку, оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий три рабочих дня с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Учреждением и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъект персональных данных не позднее трёх рабочих дней со дня уничтожения.

16.6. Уничтожение персональных данных на бумажных носителях осуществляется механическим способом. Отобранные к уничтожению документы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются. Накапливаемые для уничтожения документы, копии документов, содержащие персональные данные, хранятся отдельно.

16.7. Подлежащие уничтожению файлы, папки с персональными данными на электронных носителях уничтожаются путём, исключающим возможность последующего восстановления (удаляются средствами операционной системы компьютера с последующим «очищением корзины» или форматированием съёмного носителя).

16.8. Уничтожение пришедших в негодность электронных носителей, содержащих персональные данные, обрабатываемые в Учреждении в электронном

виде, осуществляется путём нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления данных. Вышеуказанное достигается путём деформирования, нарушения единой целостности носителя или его сжигания.

16.9. Уничтожение носителей персональных данных производится в присутствии всех членов комиссии.

17. Порядок доступа в помещения, в которых ведется обработка персональных данных

17.1. Нахождение в помещениях, в которых ведется обработка персональных данных лиц, не являющихся лицами, уполномоченными на обработку персональных данных или не имеющими доступ к персональным данным, возможно только в присутствии сотрудника, имеющего доступ к персональным данным.

17.2. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на начальников (руководителей) соответствующих отделов Учреждения.

Приложение №1 к Политике
в отношении обработки персональных данных в государственном областном автономном учреждении «Агентство развития Новгородской области»

ФОРМА

Журнал учета событий
в сфере защиты персональных данных в Учреждении

№	Наименование события (контрольное мероприятие, нарушение и пр.)	Дата события	Результаты события, принятые меры по результатам	ФИО ответственного за организацию обработки персональных данных	Примечание